COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE
500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

February 6, 2007

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

INFORMATION SECURITY STRATEGIC PLAN APPROVAL
(All Districts – 3 Votes)

IT IS RECOMMENDED THAT YOUR BOARD:

Approve and adopt the Information Security Strategic Plan for implementation within the County of Los Angeles.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The attached Information Security Strategic Plan (Plan) has been developed to provide a strategy for continuing an effective information security program for the County of Los Angeles that reduces the risk to County information and information technology (IT) assets. This Plan is designed to provide a balance between sustaining cost and the process/procedural actions taken to mitigate risks.

The purpose of the Plan is to provide an enterprise approach to information security and assist all departments in understanding and budgeting for information security systems and staff. It will be updated on an annual basis to ensure that it is kept current with changing technology and threats. It will also serve as guidance for the selection of enterprise security solutions and the establishment of annual security projects that support the implementation of the countywide strategic plan.

This Plan is also reflective of the many actions already taken to protect the IT assets, protect the information developed by and entrusted to it and assure that all County services and business processes continue to be provided as needed and without interruption due to unexpected security events.

Information Security Actions Completed to Date

- Established a Network Operations Center manned on a 24/7 basis to notify management and alert the County's information security management team of malicious activity.

- Conducted a network penetration study that identified information security weaknesses and vulnerabilities and implemented recommendations to improve detection and response effectiveness.

- Implemented a robust network intrusion detection/prevention system that monitors the County's wide area network to detect and block unwanted activities from internal and external sources.

- Implemented correlation software for the collection and analysis of data from key devices and applications that allows tracking of triggered events for critical security troubleshooting and forensics.

- Negotiated an agreement with Symantec and Network Associates, the major providers of anti-virus software, to establish a unique technical environment that enables County departments to maintain the latest anti-virus updates and technical information to combat outbreaks of malicious code.

- Established a County Computer Emergency Response Team (CERT) comprised of representatives from all County departments to respond to events on a 24/7 basis to contain and mitigate malicious attacks.

- Established countywide information security policies and procedures to promote industry security best practices.

- Implemented a comprehensive Business Continuity Program including establishing an Orange County Disaster Recovery Site to ensure the availability of time-sensitive critical services and assets in case of a major outage.

- Implemented patch management to ensure compliance with the latest software releases related to critical vulnerabilities.

- Using the Information Technology Fund (ITF) provided funding to ensure departments have the minimum level hardware devices in place that could take advantage of current security software releases.

- Developed an RFP to acquire and install encryption systems on all laptop computers.

- Developed an employee security awareness program and acquired content to be made available on the County's enterprise learning management system.

FISCAL IMPACT/FINANCING

Implementation of the strategies that are outlined in this plan will require each department to budget for additional software and staffing as needed.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

None.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

No impact.

CONCLUSION

The Information Security Strategy provides a roadmap for all departments to participate in the best security practices to protect their information assets. The office of the CIO through the Chief Information Security Officer (CISO) will provide guidance and assistance to allow departments to meet the strategic directions leading to adoption of the security recommendations. Additionally, the Plan will support enterprise solutions for the countywide acquisition of required software, implementation of enterprise access controls and assistance in coordinating County information security efforts. The annual review of this plan will ensure that it remains consistent with current technology and business needs. Development of annual security budgets will be better coordinated to meet the requirements of this plan.

Respectfully submitted,

JON W. FULLINWIDER
Chief Information Officer

JWF:DS:sjc

Attachment

c: All Department Heads

P:Drafts/Security/ISSP Approval.doc

The County of Los Angeles
Information Security Strategic Plan
Version 1.0
01/23/07

Office of the CIO
Jon Fullinwider

Acknowledgement

Development Coordination
Chief Information Security Officer and Staff
Department of the CIO, County of Los Angeles
Charles P. Meister & Ashish Soni
Institute for Critical Information Infrastructure Protection
Center for Telecom Management
Marshall School of Business
University of Southern California

THE COUNTY OF LOS ANGELES 1

INTRODUCTION: 1

EXECUTIVE SUMMARY 1

SCOPE 2

OVERVIEW 2

INFORMATION SECURITY STRATEGIC FRAMEWORK 6

Key Areas of the Strategic Framework 7

Vision Statement: 8

Mission Statement: 8

Strategic Themes/Goals: 8
Organization: 8
People: 9
Process: 9
Technology 9

STRATEGY STATEMENTS 9
Organization: 9
People: 9
Process: 10
Technology: 10

ACTION PLAN FRAMEWORK 12

COUNTY OF LOS ANGELES ACCOMPLISHMENTS AND FUTURE OBJECTIVES 48

1. Security Organization 48
Chief Information Security Officer (CISO) 49
Information Security Steering Committee (ISSC) 50
Department Information Security Officer (DISO) 50
Countywide Computer Emergency Response Team (CCERT) 50
Future Organization Activities 51

2. Compliance and Privacy 51
Privacy Legislation Status and Strategy 51

3. User Security Awareness and Training 52

Employee Awareness Status and Strategy 52
Security Awareness Activities 52

4. Policies, Standards and Procedures **53**
Security Policies Status and Strategy 53
Policy Activities 54

5. Risk Management **54**

6. Network Security and Access Controls **54**
Status and Strategy 55
Network Access Control Actions 55

7. Monitor and Audit **56**

8. Physical Protection of Information Assets **56**
Physical Protection Status and Strategy 56
Existing Environments 57

9. Business Continuity and Disaster Recovery **57**
Business Continuity Status and Strategy 57

10. Systems Implementation and Administration **57**
Desktop and Laptop Systems 58

LOS ANGELES COUNTY INFORMATION SECURITY MILESTONES AND ACCOMPLISHMENTS **59**

Milestone/Accomplishments **59**
Strategy 59

Milestone/Accomplishments **60**
Strategy 60

Milestone/Accomplishments **61**
Strategy 61

Milestone/Accomplishments **62**
Strategy 62

Milestone/Accomplishments **63**
Strategy 63

Milestone/Accomplishments **64**
Strategy 64

Milestone/Accomplishments **64**
Strategy 64

Milestone/Accomplishments **65**
Strategy 65

Milestone/Accomplishments **66**
Strategy 66

Milestone/Accomplishments **67**
Strategy 67

Milestone/Accomplishments **68**
Strategy 68

Milestone/Accomplishments **69**
Strategy 69

Milestone/Accomplishments **70**
Strategy 70

Milestone/Accomplishments **71**
Strategy 71

VI. THE INFORMATION SECURITY SCORECARD **72**

County of Los Angeles Information Security Strategy

Introduction:

The County of Los Angeles must be able to protect its computing resources and the information that is entrusted to it. To protect that information, the County must approach the process with a countywide strategy that is endorsed by the Board and supported by all County departments. Strategies must be tailored to match the business needs of the county, but will best be served by establishing a systems approach.

Information technology and its protection affect nearly every Department in the County of Los Angeles. As networked information systems and the Internet become even more pervasive and critical to our conduct of County business, it is essential that we protect our information assets to assure confidentiality, integrity and availability in that process. Moreover, risks to information systems from hackers, disgruntled insiders, cyber terrorists, viruses, and worms have never been greater. It is important that the County adopt a strategic approach to the information security process.

Executive Summary

One of the most important assets of Los Angeles County is its information. The Board of Supervisors, County Administrators, and Department Heads have legal obligations to make certain that such information is managed within the frameworks prescribed by law and regulation. The value and criticality of these informational assets require the implementation of a formal Information Security Program to meet these legal and moral responsibilities. Major goals of the Information Security Program are to enhance the productivity of Los Angeles County and the quality of life of its constituents, as well as ensure the protection and preservation of lives and systems. This is accomplished by maintaining the integrity, confidentiality and availability of the County's informational assets.

A County government is a unique business entity. This is evident when you consider the threats that government now faces (e.g., cyberspace terrorism, bio-terrorism, day-to-day hackers, unauthorized intrusions, virus attacks, etc.), the diversity of the operations of its agencies, the various governing laws and statutes, multiple sources of funding, and the interaction between elected and appointed officials throughout government. This uniqueness requires a correspondingly unique Information Security Strategy that is tailored to a local county government.

Scope

The County of Los Angeles has a very formal security program. In order to mitigate the risks of an attack on the County's information networks and protect the public's data, the County has developed a balanced plan for defending its information infrastructure that enables it to reduce information security exposures and respond appropriately to any incidents, which may occur. The County has undertaken a number of actions (see section VI for a list of Milestones), which has significantly reduced the County's exposure to Cyber threats and has put in place policies and procedures to prevent, detect, respond to and mitigate cyber threats. The County of Los Angeles Security Strategic Plan articulates the components and direction for the implementation and management of a Countywide Information Security program, which is designed to allow the ability to deliver and respond to public issues and needs from an Information Technology perspective.

Overview

Information technology has continued to undergo rapid and constant change to an extent that has not previously been seen in our nation's history. For the past two decades, there have been continual, dramatic increases in performance and functionality, accompanied by significantly decreasing prices for information technology products. This rapid change and innovation has impacted almost all businesses, government, academia, and individuals and has enabled the development of new industries, products, and services. Information technology systems are widely distributed throughout the world, and tens of millions of people have started to access information through computer networks.

The digitization of information brings a host of new applications and advances the vision of a global information infrastructure and creates one of the most exciting, promising and challenging periods in the history of technology. Digitization allows voice, text, data, images; video and multimedia to be generated processed, transmitted, stored and received in a common form or language, and thereby enables multiple functions to come together on common platforms. Increased computational power and bandwidth are leading to new applications combining multiple functions such as electronic commerce; search and retrieval of multimedia information from digital libraries, and remote medical care treatments.

Along with the technological gains, the rapid movement of business and government to highly networked information technology has brought to the front several concerns and challenges. Technology is no longer the province of the scientist and engineer, but has broader societal, legal, commercial, economic, and governmental implications. Information Security or Cyber Security is central to many, if not all, of the issues.

Government, to the extent that its role is to protect the rights of its residents and provide public service, has a clear interest to secure its assets and protect its residents' private information. This is especially true for the County of Los Angeles whose hallmarks of

government are ***Service*** that is customer-focused and offers self-service options, ***Convenience*** that provides increased access to services beyond traditional hours of operations, and ***Value*** by providing desired services in highly efficient ways. Technology is an enabler to support the County Vision: *"To enrich lives through caring and effective service"* and is based on Information Technology infrastructure.

The informational assets of Los Angeles County include all data, in any form, and all data systems located anywhere within its individual departments and other organizations. The diversity of these assets, and the foreign and domestic threats to them, further complicate the task of information security. Information security is a never-ending process since technology continues to evolve and therefore, requires a sustained commitment from everyone involved and at all levels in the organization. Threats to County systems also continue to evolve with changes in business requirements. Multiple factors affect an organization's response to threats including government regulations and business objectives as surveyed by Ernst and Young's 2005 Global Information Security Survey.

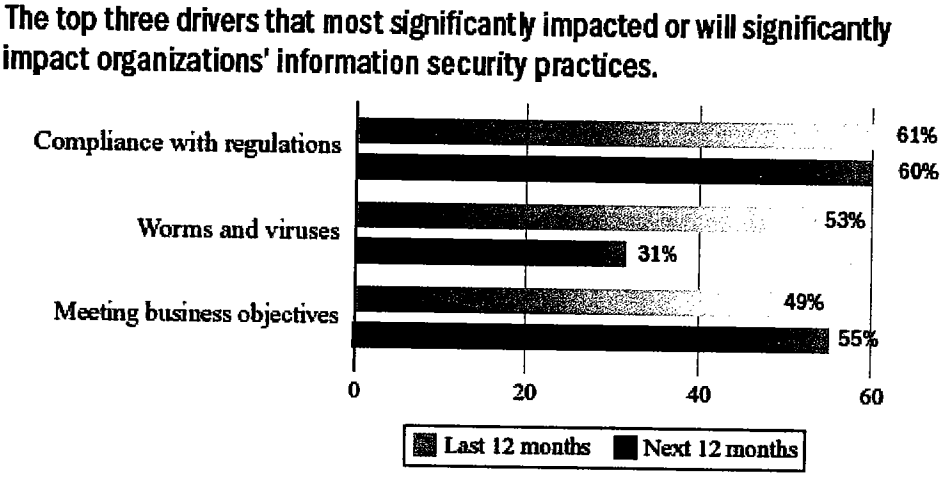

Figure 1

The County of Los Angeles has the same concerns as those listed in Figure 1 that require the application of information security resources. Currently, the County is subject to the Health Insurance Portability and Accountability Act (HIPAA) and is actively pursuing solutions to ensure compliance. There are very serious implications to the County as well as its patients if unauthorized access or if unauthorized modifications were made.

There have been numerous incidents of the exposure of private information by organizations and identity theft is one of the fastest growing crimes in the country. From a County standpoint, if criminal records from the District Attorney, Sheriff or Probation offices were accessed, lives could be lost or criminals released prematurely. If records from electronic commerce transactions or employee data are exposed, financial

reputations could be affected. It is clear that a breach in the security of some of these informational assets could have very serious consequences to the County as well as to people whose information is maintained within the County information systems.

Legislation will continue to be introduced to protect the privacy of personal information by businesses. This legislation will apply to the County as well as other levels of government and private industry. The County is similar to other organizations with needs that cause management to emphasize the importance of controls for different reasons. As the following Ernst &Young graphic demonstrates, there are multiple drivers of information security practices that will require enterprise approaches.

Top regulations or requirements that impact organizations' information security practices.

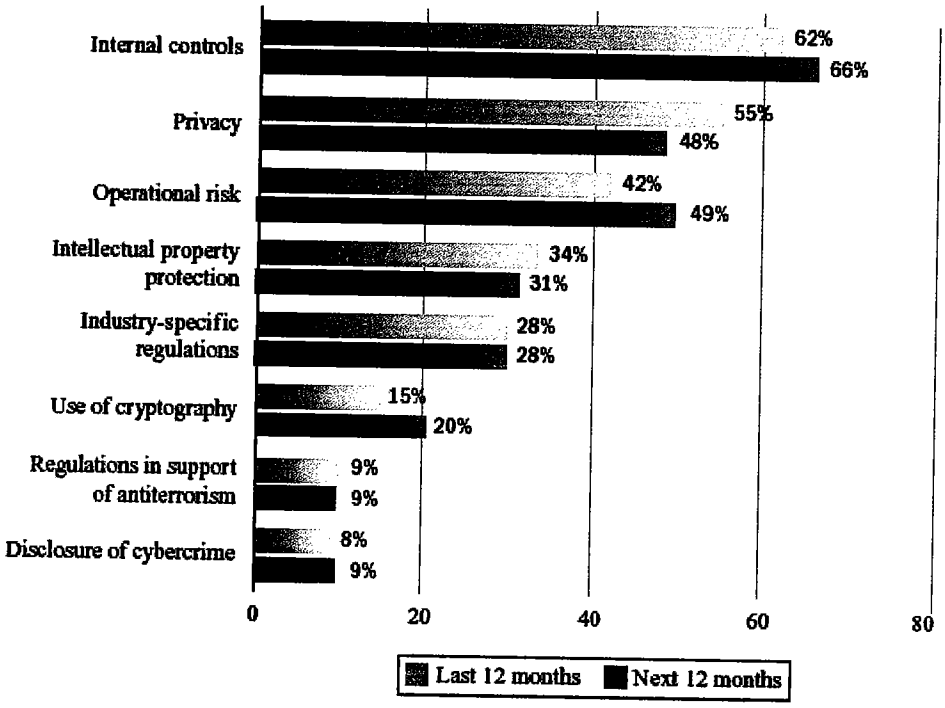

Figure 2

Security solutions must be developed to support evolving business requirements. These requirements will be affected by the emergence and availability of new technologies that can be used to provide business solutions. The County will continue to implement new technologies that provide cost effective solutions to County needs. This includes emerging technologies such as Voice over IP (VoIP), wireless communications including wireless local area networks (WLAN), Linux (open source) systems and portable technologies.

An important strategic direction of information security in the County of Los Angeles is to support the use of new technologies and provide security measures that can assist in secure implementation. This is particularly true of wireless systems that provide enhanced access to the county networks. That access must be carefully implemented to

ensure that only authorized users are allowed to access IT assets, that privacy of County information is maintained and that networks are protected from the introduction of malicious computer code. VoIP technologies provide a cost effective alternative to traditional telephone technologies, but can be affected by denial of service attacks and connection of rogue devices. Security measures must be designed to mitigate against these risks. Many of the existing information security protection measures will assist in the secure implementation of new technologies, but they must be augmented with technology specific applications to provide maximum cost effective security measures. Figure 3 illustrates the new technologies that will drive security efforts in the coming years.

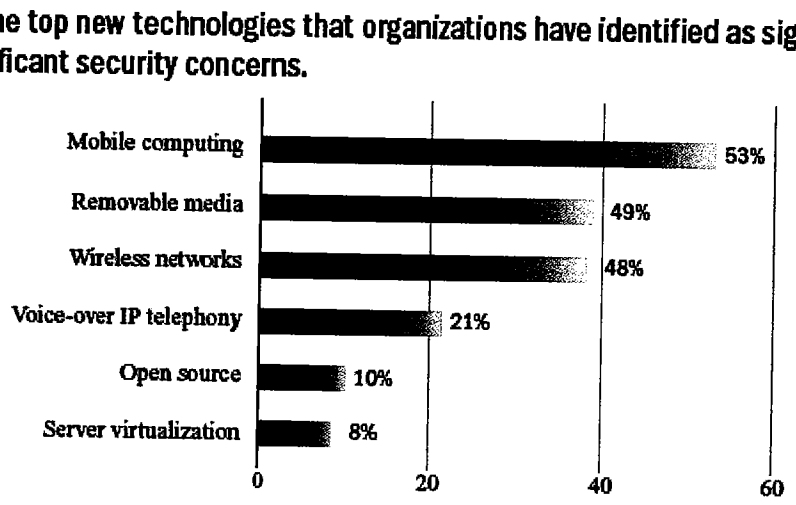

Figure 3

As shown in the above figures, there are multiple drivers to developing information security in the County of Los Angeles. None of these drivers or requirements can be addressed on a stand alone basis, but must be part of a comprehensive approach. It is also clear that the County cannot take a short term view of security, but must approach it strategically. The comprehensive approach must take into account the people using the systems, the technology being employed and the business processes that drive them. This strategy document specifies that strategy and enumerates actions that have already been completed.

Information Security Strategic Framework

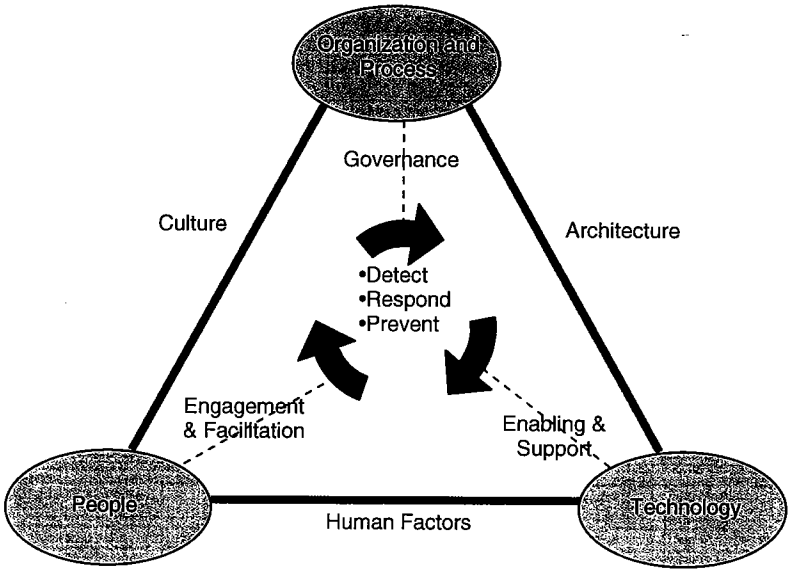

Figure 4

The Information Security Strategic Framework developed to support the County is designed to address organization, people, processes and technology as they relate to information security. The Strategy is based on the principle that security is not a one-time event, but must be a continuously improving process, an emergent process that addresses changes in business requirements, technology changes and new threats and vulnerabilities and a need to maintain currency with regard to software release levels at all levels within the security network/server client arena. It also is based on the realization that perfect security is an impossible goal and that efforts to secure systems must be based on cost of protective measures versus risk of loss.

The County of Los Angeles has taken a proactive and pragmatic approach towards information security during the past few years. This approach requires deploying key technologies and establishing best practices to achieve business value in terms of sustained productivity and regulatory compliance. The overall IT industry and its customers have grown more sophisticated in dealing with security vulnerabilities, utilizing matured and integrated systems to protect their environments. The Strategy calls for the county to adopt a balanced position to information security investment, weighing the cost of additional security measures with potential breeches to match the tolerance of risk for the enterprise as Figure 5 illustrates.

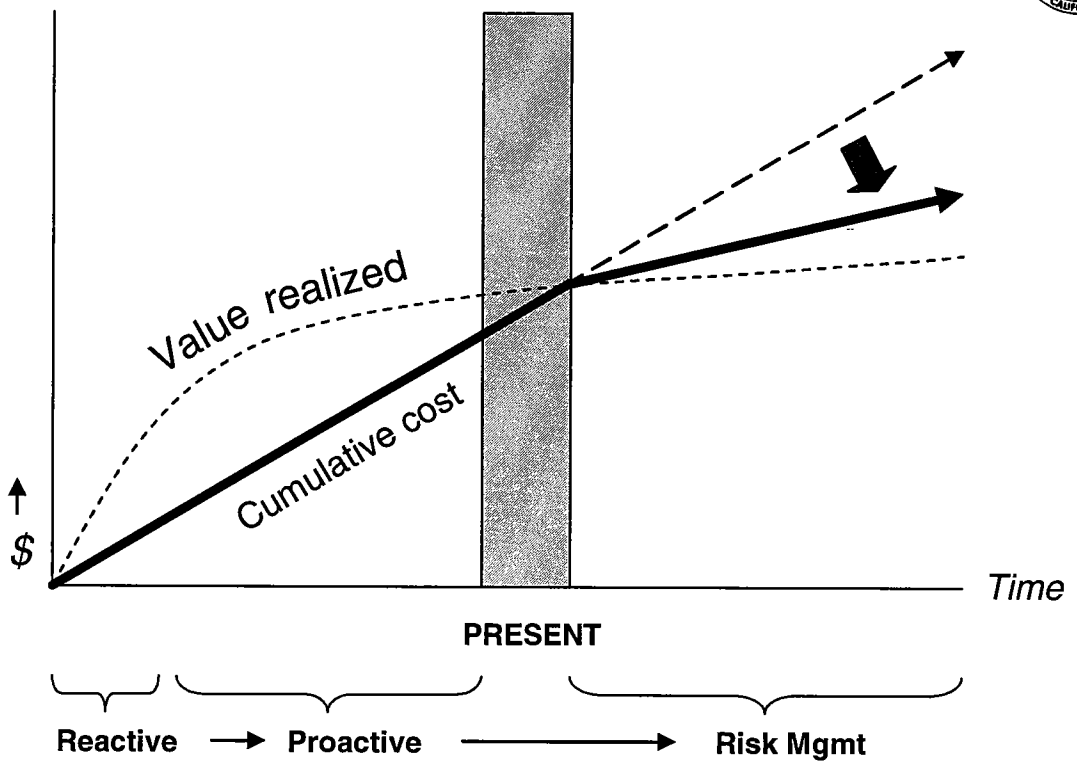

Figure 5

Key Areas of the Strategic Framework

This Strategic Framework is organized according to the following 12 key Information Security areas as defined by the County CISO:

1. Security Management and Organization
2. Compliance and Privacy
3. User Security Awareness and Training
4. Policy, standards and procedures
5. Risk Management
6. Access Control
7. Monitor and Audit
8. Physical Security
9. Business Continuity Planning and Disaster Recovery
10. Application and Systems Development
11. System Architecture and Design
12. System and network Management

The basis for security strategy approaches is that they are designed to be proactive to information security rather than reactive. Preventive measures are more cost effective than actions required after breaches have occurred. However, when events do occur, the

strategic approach must include capabilities to respond, mitigate and recover from the incidents. In order to mitigate the risks of an attack on the County's information networks and protect the public's data, the County will implement a balanced plan for defending its information infrastructure that will enable it to reduce information security exposures and respond appropriately to any incidents, which may occur.

For all goals, strategies, objectives and activities the County will partner as a statewide community with government at all levels, the private sector, associations, and organizations to ensure a safe and secure technical state for our residents. The matrix presented on the following pages outlines our goals, objectives and strategies, which are part of the strategic planning framework linkage that transforms the countywide vision and mission into action. Goals represent what the county must achieve within each theme/perspective in order to achieve the vision and mission. Objectives further define goals into specific steps or end states for goal accomplishment. Strategies define what must be done to accomplish goals that support the county mission and vision within each area.

Vision Statement:

The County will take a balanced approach to provide protection of information assets to ensure their confidentiality, integrity and availability.

Mission Statement:

The County Information Security Mission is to secure the county systems and information assets that are required to provide services to its residents.

Strategic Themes/Goals:

Strategic themes are part of the Framework that translates the countywide vision and mission into action. Themes dissect the strategic priorities and organize them into topic areas in which the county must excel if it is to accomplish their Information Security Mission and Vision. Defined by the 4 key areas of the overall framework, the following Themes/Goals were determined to support the vision and mission of the County:

Organization:

Common and Co-operative Approach:
Develop a dynamic county wide information security program that applies to all departments and provides a common and co-operative approach to information security and implements best practices reflected in industry and government.

People:

Sustained Commitment:
Ensure that the users of county information assets understand the value of protecting those assets that are entrusted to them and the methods to do that by ensuring that the security program is communicated to all users.

Process:

Balanced and Effective Approach:
Implement enterprise policies, standards, procedures, toolsets and systems to ensure the

- Ability to prevent, detect, respond and mitigate information security incidents.
- Viability of the protective measures and,
- Measurement of the progress of the information security program

Technology

Standardized, Cost-effective and Current:
Maintain security and currency of software, hardware and information assets.
Develop and establish standards for implementing and maintaining information security.

Strategy Statements

Organization:

1. **Security Management and Organization**
   Establish a focal point for information security program development responsible for creating a countywide collaborative framework to encourage individual department participation.

2. **Compliance and Privacy**
   Develop measures to implement best security business practice and provide privacy of information entrusted to the county and comply with legislation.

People:

1. **User Security Awareness and training**
   Provide security awareness training to establish accountability for user actions, train for accountability and enforce it, as reflected in organizational policies and procedures. Provide specialized training for security staff and people is critical positions.

Process:

1. **Policy, Standards and Procedures**
   a. Provide a comprehensive, documented information security policy which should be communicated to all individuals with access to the County's information and systems.

2. **Risk Management**
   a. Conduct a periodic information security risk evaluation that identifies critical information assets (e.g., systems, networks and data), threats to critical assets, asset vulnerabilities, and risks.

3. **Access Control (authentication and authorization)**
   a. Implement and maintain appropriate mechanisms for user authentication and authorization when using network and system access from inside and outside the organization.

4. **Physical Security**
   a. Control physical access to information assets and IT services and resources.

5. **Business Continuity Planning & Disaster Recovery**
   a. Develop business continuity and disaster recovery plans for critical assets and ensure that they are periodically tested and found effective.

6. **Applications, Systems Development and Procurement**
   a. Develop methodologies to ensure that information security is built into and periodically tested within the development and operational phases of software applications.
   b. Develop processes to review and certify purchased software prior to implementation in the County environment.

Technology:

1. **Security Architecture & Design**
   a. Generate, implement, maintain and document countywide security architecture, based on standards that satisfy County business objectives while protecting critical information assets.

2. **System & Network Management**
   a. Establish a set of security controls to protect assets residing on systems and networks including access control, software integrity, secure asset configuration and backups.

3. **Monitor & Audit**

a. Use appropriate monitoring, auditing, and inspection facilities and assign responsibility for reporting, evaluating, and responding to system and network events and conditions.

Action Plan Framework

Strategy	Objectives	Activities
1. Security Management and Organization	**1.1 Information Security Function** a specialist information security function should be established, which has countywide responsibility for promoting information security.	**1.1.1** The Chief Information Security Officer (CISO) under the direction of the CIO will: • Co-ordinate information security across the county. • Develop and maintain a current information security strategy. • Provide information security-related technical, regulatory and policy leadership. • Facilitate the implementation of County information security policies. • Coordinate information security efforts across departments. • Lead continuing information security training and education efforts. • Serve as an information security resource to department heads and the Board of Supervisors. • Establish a joint interdepartmental steering committee. • Investigate major information security incidents. • Monitor the effectiveness of information security. **1.1.2** The information security function should be adequately resourced in terms of the number of staff, their range and level of skills, education, certifications and relevant tools or techniques. **1.1.3** Designate a County organization that will be funded and staffed to provide

		solutions to county Information Security initiatives under the direction of the CISO. **1.1.4** Financial costs associated with information security activities across the County will be identified, understood and adequately funded.
	1.2 Interdepartmental Collaboration The CISO will coordinate information security activity in business units/departments to ensure that security activities are carried out in a timely and accurate manner, county-wide, and that security issues are resolved effectively.	**1.2.1** Local information security coordinators (Department Information Security Officers) should be appointed to co-ordinate information security throughout the county. **1.2.2** Form an interdepartmental Information Security steering committee which will be composed of the Departmental Information Security Officers, the CISO and the Assistant CISO. This will provide a forum for all information security related collaboration, information sharing and decision-making. An effective security program should have open collaboration and information sharing across various County departments.
2. Compliance and Privacy	**2.1 Information Privacy** Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.	**2.1.1** A high-level committee (or equivalent) should be established to be responsible for managing information privacy issues, and an individual appointed to co-ordinate information privacy activity. **2.1.2** There should be documented standards/procedures for dealing with information privacy, which should cover: • Acceptable use of personally identifiable information. • The rights of individuals about whom personally identifiable information is held. • Privacy assessment, awareness and

		compliance programs. • Legal and regulatory requirements for privacy. **2.1.3** Where personally identifiable information is stored or processed, there should be processes to ensure that it is: • Adequate, relevant and not excessive for the purposes for which it is collected. • Accurate. • Kept confidential, processed fairly and legally, and used only for specified, explicit and legitimate purposes. • Requirements for handling personally identifiable information. **2.1.4** Personally identifiable information should be handled in accordance with relevant legislation, such as the US Health Insurance Portability and Accounting Act (HIPAA). **2.1.5** An individual (or group) throughout the enterprise should: • Perform a privacy assessment to determine the level of compliance with relevant legislation and internal policies. • Implement a privacy compliance program.
Strategy	**Objectives**	**Activities**
3. User Security awareness and training	**3.1 Security Awareness Training** To ensure all county employees understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.	**3.1.1** The security awareness and education activities should be: • Endorsed by top management • Supported by a documented set of objectives. • Delivered as part of an on-going security awareness program. • Kept up-to-date with current practices and requirements.

		• Aimed at reducing the frequency and magnitude of incidents that are measurable. **3.1.2** Security awareness should be promoted: • To top management, business managers/users, IT staff and external personnel. • By providing information security education/training, such as via computer-based training (CBT). • By supplying specialized security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents. **3.1.3** The effectiveness of security awareness should be monitored by measuring: • The level of security awareness in staff and reviewing it periodically • The effectiveness of security awareness activities, for example by monitoring the frequency and magnitude of incidents experienced. **3.1.4** Security-positive behavior should be encouraged by: • Making attendance at security awareness training compulsory • Mandatory inclusion in new employee orientation • Linking security to personal performance objectives/appraisals.
	3.2 Security Education Staff should be educated in how to run systems correctly and how to develop and apply security controls.	**3.2.1** Training should be given to provide IT staff with the skills they need to: • Assess security requirements. • Propose security controls. • Ensure that security controls function effectively in the environments in which

		they are applied. **3.2.2** Education/training should be carried out to provide: • Systems development staff with the skills they need to design systems in a disciplined manner and develop security controls. • IT staff with the skills they need to run computer installations and networks correctly and apply security controls. • Information security specialists with the skills they need to understand the business, run security projects, communicate effectively, and perform specialist security activities. **3.2.3** A County certification program in information security should be developed and made available to county technology staff members.
Strategies	**Objectives**	**Activities**
4. Policy, standards and procedures	**4.1 Security Policy** A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.	**4.1.1** The CISO in conjunction with the departmental representatives will develop a comprehensive set of Information Security and technology policies which will be approved by the board of supervisors and applicable to all county organizations as a minimum standard. **4.1.2** The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff. **4.1.3** Create policies that address key security topic areas such as security risk management, critical asset identification, physical security, system and network management, authentication and authorization, access control, vulnerability management, incident management, awareness and training, and

		privacy. **4.1.4** The information security policies should be reviewed on an annul basis. **4.1.5** The following list of policies should be created by the County to address Information Security issues: • Acceptable Use policy • Antivirus policy • Auditing and Compliance policy • Internet Usage Policy • Electronic Email Policy • Physical Security Policy • Risk Assessment Policy • Threat Response policy • Business Continuity Policy • Data Disposal Policy • Software Security Policy • Portable Device Security Policy • Data classification policy • Incident Response policy • Network Security Policy • Training and Awareness Policy
5. Risk Management	**5.1 Risk management** Critical applications, computer installations, networks and systems under development should be subject to a formal risk analysis on a periodic basis.	**5.1.1** There should be documented standards/procedures for risk analysis that apply across the County, which should require risks to be analyzed for: • Information and systems that are critical to the County. • Vulnerabilities related to non-critical systems • New systems at an early stage in their development. • Systems subject to significant change, at an early stage in the change process. • The introduction of major new technologies. • Requests to permit access to the County's information and systems from external locations or by third parties. • Live systems that were implemented

		before the introduction of risk analysis processes. **5.1.2** Standards/procedures should require that risk analysis: • Is performed periodically. • Is performed prior to implementation of new systems • Involves representatives from key areas, including IT specialists, key user representatives and experts in risk analysis and information security. **5.1.3** Business risks associated with the County's information and systems should be analyzed using formal risk analysis methods, which should be: • Documented. • Consistent across the County. • Reviewed periodically to ensure that they meet the County's business needs. • Applicable to systems of various sizes and types. **5.1.4** Risk analysis methods should include a process to ensure that the results of the risk analysis are documented and include: • A clear identification of key risks • An assessment of the potential business impact of each risk. • Recommendations for actions to reduce risks to acceptable levels.
6. Access Control	**6.1 User authentication** Implement and maintain appropriate mechanisms for user authentication and authorization when using network access from inside and outside the organization.	**6.1.1** Users of County Information Systems should be identified, authenticated and authorized. **6.1.2** System administrators should be subject to strong two factor authentication. **6.1.3** There should be a method of ensuring

		that users do not share identification or authentication details. **6.1.4** There should be a process for issuing new or changed passwords that: • Ensures that passwords are not sent in the form of clear text e-mail messages. • Directly involves the person to whom the password uniquely applies. **6.1.5** Users' access rights should be: • Restricted according to a defined policy, such as on a 'need to know' or 'need to restrict' basis. • Restricted according to users' individual roles. • Revoked promptly when an individual user is no longer entitled to them. • Enforced by automated access control mechanisms to ensure individual accountability. **6.1.6** Access to the application should be logged. Access logs should include sufficient information to provide a satisfactory audit trail. **6.1.7** County should strive and plan to migrate to strong authentications mechanisms including certificates.
	6.2 User authorization All users should be authenticated by using User IDs and passwords or by strong authentication mechanisms before they can gain access to target systems.	**6.2.1** All users of the County's systems should be subject to an authorization process before they are granted access privileges. **6.2.2** The processes for authorizing users should be documented. **6.2.3** A database containing details of all authorized users should be established, which should be maintained by designated individuals, such as particular system administrators, and protected against

		unauthorized change or disclosure. **6.2.4** Details of authorized users should be reviewed: • To ensure that access privileges remain appropriate. • To check that redundant. authorizations have been deleted • To delete access for terminations and transfers. • On a regular basis. • On a more regular basis for users with special access privileges.
	6.3 Third party access Connections from third parties should be uniquely identified, subjected to a risk analysis, approved, and supported by contracts.	**6.3.1** The provision of third party access should be supported by documented standards/procedures, which should specify that, prior to connection: • The business risks associated with third party access are assessed. • Agreed security controls are implemented. • Testing is performed. **6.3.2** There should be a process in place to: • Protect the interests of the County in relation to ownership of information and systems. • Limit the liabilities of the County to third parties. • Comply with regulatory/statutory obligations. • Make third parties accountable for their actions. **6.3.3** When dealing with individual third party connections, there should be a process in place to: • Restrict methods of connection. • Authenticate users in line with the type of access granted. • Restrict the type of access granted. • Grant access to the County's information and systems on the principle of 'least

		access'. • Achieve technical compatibility using standards. • Protect sensitive information stored on target systems or in transit to third party locations. • Log activity. • Terminate connections when no longer required.
7. Monitor and Audit	**7.1 Security Monitoring** The information security condition of the County should be monitored periodically.	**7.1.1** There should be arrangements for monitoring the security condition of the County, which should be defined in writing and performed periodically. **7.1.2** Monitoring arrangements should: • Keep County CIO and CISO informed of key risks. • Focus on business-critical information and systems. • Cover all parts of the County. • Collect information in a quantitative, standard format. **7.1.3** Information collected for monitoring purposes should include details about: • The criticality of information and systems. • Threats from accidents and deliberate acts. • The full range of controls needed to protect the confidentiality, integrity and availability of information and systems. • The status of controls applied. • Vulnerabilities caused by control weaknesses and special circumstances that increase vulnerability, such as major changes to systems. • The pattern and business impact of incidents. • Individual incidents that have had a severe business impact on the County. • The cost of security controls. **7.1.4** A Security Dashboard should be

		established that will provide a snapshot of the status of the County security and provide updates on county information security initiatives. **7.1.5** The CISO should establish effective metrics to monitor the effectiveness of County cyber security initiatives.
	7.2 Security Audit The information security status of critical IT environments should be subject to thorough, independent and regular security audits/reviews	**7.2.1** Independent security audits/reviews and vulnerability scans should be performed periodically for critical environments, including business applications, computer installations, networks, systems development activities and key countywide security activities. **7.2.2** Security audits/reviews should be: • Defined in scope, and documented. • Performed by qualified individuals who have sufficient technical skills and knowledge of information security. • Conducted sufficiently frequently and thoroughly (in terms of scope, extent) to provide assurance that security controls function as required. • Focused on ensuring that controls are effective enough to reduce risks to acceptable levels. • Supplemented by the use of automated software tools. • Complemented by reviews conducted by independent third parties.
	7.3 Incident Management All incidents – of any type – should be recorded, reviewed and resolved using an incident Management process.	**7.3.1** All incidents that affect the application (including malicious attacks, abuse/misuse of systems by staff, loss of power/communications services and errors by users or computer staff) should be dealt with in accordance with an incident management process. **7.3.2** The incident management process

		should be documented, and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents and escalation processes. **7.3.3** Incidents should be: • Reported to a single point of contact, such as a help desk, telephone hot line or individual IT specialist. • Documented, typically using an automated incident management system. • Categorized by type. • Prioritized according to their impact/urgency. **7.3.4** The resolution of incidents should include: • Investigating their root causes. • Planning corrective action to ensure security is not affected. • Restricting access when corrective actions are performed. • Documenting corrective actions taken • Performing a review to ensure that the security of the application has not been affected by the incident or its resolution. **7.3.5** Patterns of incidents should be reviewed to identify potential security breaches and minimize the chances of similar incidents disrupting the application – or other applications – in the future. **7.3.5** Incident Response training programs should be developed and given to IT staff members with the skills they need to detect and respond to incidents.
	7.4 Forensic Investigations A process should be established for dealing with incidents that require forensic investigation.	**7.4.1** There should be documented standards/procedures for dealing with incidents that may require forensic investigation, which should cover: • Immediate preservation of evidence on

		discovery of an incident. • Compliance with a published standard or code of practice for the recovery of admissible evidence. • Maintenance of a log of evidence recovered and the investigation processes undertaken. **7.4.2** Co-ordinate efforts with Auditor Controller to handle cyber security incidents and to investigate computer crime.
8. Physical Security	**8.1 Hazard Protection** Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards to prevent services from being disrupted by damage to computer equipment or facilities.	**8.1.1** The computer installation should be located safely and in rooms that are protected from natural hazards. **8.1.2** Rooms housing critical IT facilities should be: • Free from intrinsic fire hazards (such as paper or chemicals). • Fitted with fire detection and suppression systems. • Protected against the spread of fire. • Fire alarms should be monitored constantly, tested periodically and serviced in accordance with manufacturers' specifications. **8.1.3** The impact of hazards should be minimized by: • Locating hand-held fire extinguishers so that minor incidents can be tackled without delay • Protecting computer equipment against damage from environmental hazards (e.g. smoke, dust, vibration, chemicals, electrical interference/radiation, food, drink and nearby industrial processes) • Monitoring and controlling the temperature and humidity of computer rooms in accordance with recommendations from equipment manufacturers.

	8.2 Physical Protection All buildings throughout the County that house critical IT facilities should be physically protected against accident or attack to restrict physical access to authorized individuals and ensure that IT facilities processing critical or sensitive information are available when required	**8.2.1** There should be documented standards/procedures for the provision of physical protection in areas housing IT facilities. **8.2.1** Standards/procedures should include the protection of: • Buildings against unauthorized access • Important papers and removable storage media against theft or copying • Easily portable computers and components against theft • Recording access to the facilities through electronic access control **8.2.2** Buildings that house critical IT facilities should be protected against unauthorized access by: Providing locks, bolts or equivalent on vulnerable doors and windows • Employing security guards • Installing closed-circuit television. **8.2.3** Important papers and removable storage media should be protected against theft or copying by: • Storing sensitive physical material in locked cabinets (or similar) when not in use • Restricting physical access to important post/fax points • Locating equipment used for sensitive printed material in secure physical areas. **8.2.4** Easily portable computers and components should be protected against theft by using physical locks and indelibly marking vulnerable equipment. **8.2.5** Use full disk encryption on laptop computers and encrypt sensitive information that is stored on portable computing devices.
	8.3 Power Supplies Critical computer equipment	**8.3.1** Power cables within the computer

	and facilities should be protected against power outages to prevent services provided by the computer installation from being disrupted by loss of power	installation should be protected by: • Segregating them from communications cables to prevent interference. • Concealed installation. • Locked inspection/termination points • Alternative feeds or routing. **8.3.2** The power supply to critical computer equipment should be protected by: • Fitting uninterruptible power supply (UPS) devices. • Providing back-up generators in case of extended power failure. • Installing emergency lighting in case of main power failure. • Placing emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency.
9.Business Continuity Planning and Disaster Recovery	**9.1 Availability requirements** The County will document and define the availability requirements, i.e. the need for information to be accessible when required, of a given application by assessing the impact on County operations of information stored in or processed by the application being unavailable for any length of time. **9.2 Backup Strategy** To ensure that, in the event of an emergency, essential information and software required by the installation can be restored within critical timescales, essential	**9.1.1** The impact of business information stored in or processed by the application being unavailable for any length of time should be assessed in terms of: • Potential damage to public image and reputation • The possibility of incurring additional costs • A breach of legal, regulatory or contractual obligations • The potential disruption of County business activity. **9.1.2** The critical timescale of the application should be determined. **9.2.1** Back-ups of essential information and software should be taken frequently enough to meet County business requirements. **9.2.2** Back-ups should be: • Performed using a back-up management process

	information and software used by the computer installation will be backed up on a regular basis, according to a defined cycle.	• Documented and verified to ensure that back-up versions can be restored successfully. **9.2.3** Back-up arrangements should enable software and information to be restored within the critical timescale of the application. **9.2.4** Back-ups should be protected from loss, damage and unauthorized access, by: • Storing them in a fireproof safe on-site, to enable important information to be restored quickly. • Supporting them by copies kept off-site, to enable required systems to be restored using alternative facilities in case of a disaster. • Restricting access to authorized staff. • Designating alternate staff for critical operations.
	9.3 Business Continuity Planning In order to enable the county to withstand the prolonged unavailability of critical information and systems, the County will establish documented standards/procedures for developing business continuity plans and for maintaining business continuity arrangements throughout the county.	**9.3.1** A formal process for developing business continuity plans and maintaining business continuity arrangements across the County should be established. **9.3.2** A business impact analysis (BIA) should be conducted to assess the impact of potential disasters to county assets. **9.3.3** There should be documented standards/procedures for the development of business continuity plans, which should specify that plans are: • Provided for all critical parts of the enterprise. • Based on the results of a documented risk analysis. • Distributed to all individuals who would require them in case of an emergency. • Kept up-to-date and subject to standard change management practices.

		• Backed-up by a copy held at an off-site location. **9.3.4** The business continuity plan should contain: • A list of services to be recovered, in priority order. • A schedule of key tasks to be carried out, identifying responsibilities for each task. • Procedures to be followed in completing key tasks and activities, including emergency, fall-back and resumption procedures. • Sufficient detail so that they can be followed by individuals who do not normally carry them out. **9.3.5** There should be documented standards/procedures for the provision of business continuity arrangements, which require that arrangements cover the prolonged unavailability of: • Systems or application software. • County business information (in paper or electronic form). • Computer, communications and environmental control equipment. • Network services. **9.3.6** Ensure that business continuity arrangements are tested periodically, using realistic simulations, to demonstrate whether services can be resumed within critical timescales
10. Application and Systems Development	**10.1 Development methodologies** Development activities should be carried out in accordance with a documented system development methodology	**10.1.1** There should be a documented systems development methodology, which should ensure that systems are developed to comply with countywide security policy, legal and regulatory requirements and particular business requirements for security.

	to ensure information security.	**10.1.2** The systems development methodology should include information security considerations during definition of requirements, design and build activity, the testing process and implementation activity. **10.1.3** Development staff should be trained in how to use the systems development methodology effectively. **10.1.4** The systems development methodology should be kept up-to-date. **10.1.5** Compliance with the systems development methodology should be monitored at key stages in the systems development lifecycle.
	10.2 Development Environments System development activities should be performed in specialized development environments, isolated from the live environment, and protected against disruption and disclosure of information to provide a secure environment for system development activities.	**10.2.1** One or more system development environments should be established, in which development activities can be performed. **10.2.2** Development environments should be isolated from live environments and acceptance testing separated from development activity. **10.2.3** Development environments should be protected by: • Preventing development staff from making unauthorized changes to live environments. • Applying strict version control over system development software • Employing anti-virus software to reduce the threat of viruses. • Preventing malicious mobile code from being downloaded into development environments. **10.2.4** Key assets within development environments should be protected against unauthorized access, including software

		under development, business information used in the development process and important system documentation.
	10.3 Software System Design Information security requirements for the system under development should be considered when designing the system to produce an operational system based on sound design principles which has security functionality built-in and enables controls to be incorporated easily.	**10.3.1** The system design phase should: • Consider the full range of security controls. • Identify specific security controls required by particular business processes supported by the system under development. • Evaluate how and where security controls are to be applied. • Document security controls that do not fully meet requirements. • Include reviewing designs to ensure security controls are in place. • Specify a system architecture that can support the technical system requirements. **10.3.2** Systems should be designed to: • Provide 'defense in depth', to avoid relying on one line of defense or one type of security control. • Assume input from external systems is insecure as it might be an 'attack'. • Evaluate the defaults in all software configurations and ensure they are secure. . • Ensure key components 'fail securely'. • Run with 'least privilege', so that applications do not run with high-level privileges. **10.3.3** The evaluation of alternative designs for the system under development should take into account the: • Need to integrate with the existing information security architecture. • Capability of the organization to develop and support the chosen technology.

		• Cost of meeting security requirements. • Skills needed to develop required security controls. **10.3.4** Before coding or acquisition work begins, system designs should be documented, verified to ensure that they meet security requirements, reviewed by a specialist in information security and signed-off by the person in charge of the system(s) under development.
	10.4 Application Controls The full range of application controls should be considered when designing the system under development.	**10.4.1** The system design phase should include an assessment of possible application controls. **10.4.2** The assessment should include security controls associated with the validation of: • Information entered. • Automated processes. • Information integrity – the completeness, accuracy and validity of information. • Information output. • Changes to information. **10.4.3** The assessment should include security controls associated with the: • Detection of unauthorized or incorrect changes to information. • Use of automated 'checksum' tools or reconciliation back to source. • Protection of information from being accidentally overwritten. • Prevention of important internal information from being disclosed, such as via application responses or error messages. • Provision of error and exception reports. • Maintenance of audit trails.
	10.5 System Build	**10.5.1** System build activities (such as

	System build activities (including coding and package customization) should be carried out in accordance with industry best practices, performed by individuals provided with adequate skills/tools and inspected to identify unauthorized modifications or changes which may compromise security controls.	programming, creating web pages, customizing packages or defining data structures) should be carried out in accordance with documented standards/procedures. **10.5.2** Standards/procedures should specify: • Approved methods of building systems. • Mechanisms for ensuring systems comply with good practice for system build. • 'Secure' methods of making changes to the base code of software packages. • Review and sign-off processes. **10.5.3** System build activities should be inspected to identify unauthorized modifications or changes which may compromise security controls, and be documented. **10.5.4** When building systems: • Staff should comply with best practices for system coding • Automated tools should be used to ensure adherence to programming standards. **10.5.5** Where modifications have to be made to the base code of software packages, a documented process should be applied, which takes account of the risk of: • Built-in security controls being compromised • Incompatibility with updated versions of the base software package.
	10.6 Web enabled development Specialized technical controls should be applied to the development of web-enabled applications.	**10.6.1** Additional controls should be employed when developing systems that will support web-enabled applications. **10.6.2** The business practices and privacy policies applicable to the web site(s) that will support the application under

		development should be independently accredited. **10.6.3** The build process should ensure that the web server(s) that will support the Internet facing application will be: • Located in a 'Demilitarized Zone' (DMZ) – an area that is isolated from the Internet and other internal networks by firewalls • Run on one or more dedicated computers • Run with 'least privileges' • Prevented from initiating network connections to the Internet • Configured so that scripts can only be run from specified locations. **10.6.4** The build process should ensure that connections between web servers and back-office systems will be: • Protected by firewalls. • Restricted to those services that are required by the application. • Restricted to code generated by web server applications, rather than by client applications. • Based on documented and standardized application programming interfaces (APIs) • Supported by mutual authentication. **10.6.5** The build process should ensure that web site content will be: • Stored on a separate partition/disk from the operating system. • Protected by setting file permissions. • Updated by particular individuals and via approved methods. • Reviewed to ensure that it is accurate, that hyperlinks are valid and functional. **10.6.6** Transaction processing monitors

		should be used to manage the execution, distribution and synchronization of transactions. **10.6.7** Sensitive data in transit should be protected against disclosure by using encryption.
	10.7 Testing All elements of a system (i.e. application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.	**10.7.1** There should be a process for testing the system(s) under development, which should be supported by documented standards/procedures. **10.7.2** Standards/procedures should cover: • The types of hardware, software and services to be tested. • The use of test plans, including user involvement. • Key components of the testing process. • Documentation, review and sign-off of the testing process. **10.7.3** Key components of new systems should be tested before being installed in the live environment, including application software packages, systems software, hardware, communications and environmental services. **10.7.4** New systems should be tested in accordance with pre-defined, documented test plans, which should be cross-referenced to the system design/specification to ensure complete coverage. **10.7.5** Tests should cover: • Error situations. • Vulnerability to attack. • The impact of bad data. • Interfaces with other systems. • Compatibility with a wide range of possible workstation configurations. • The effectiveness of security controls. • Identification of maximum system capacity.

	10.8 Acquisition Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.	• System performance when handling planned volumes of working. **10.7.6** Automated tools should be used to improve the testing process, for example to check the validity of system interfaces or simulate loading from multiple clients. **10.8.1** The acquisition of hardware/software should be in accordance with documented standards/ procedures, which apply to computer/communications equipment, application packages, systems software and specialized security products. **10.8.2** Standards/procedures should specify: • Guidelines for selecting hardware/software. • Methods of identifying and addressing security weaknesses in hardware/software. • Requirements to meet software licensing obligations. **10.8.3** The likelihood of security weaknesses in hardware/software should be reduced by: • Considering external security ratings of third party products. • Published security ratings, such as the 'Common Criteria'. • Identifying security deficiencies. • Considering alternative methods of providing the required level of security. **10.8.4** The acquisition of products should be reviewed by staff that have the necessary skills to evaluate the security implications, and be approved by the person in charge of the system(s) implementation. **10.8.5** Standard language should be developed for software procurement contracts to:

		• Address remediation of security flaws discovered in standard software. • Address remediation of security flaws in modifications to standard software. • Scanning of software prior to implementation.
Strategies	**Objectives**	**Activities**
11. System Architecture and Design	**11.1 Security Architecture** The CISO will establish an 'information security architecture' for the County that will provide the basic framework for the application of standard security controls in all departments.	**11.1.1** The 'information security architecture' should be: • Applied to live systems/networks countywide. • Used in developing new applications. • Documented. **11.1.2 There** should be a countywide process for implementing coherent and consistent security mechanisms and establishing common user and application interfaces. **11.1.3** Arrangements should be made enterprise-wide to: • Minimize the diversity of hardware/software in use. • Provide consistent security functionality across different hardware/software platforms. • Integrate security controls at application, computer and network level. • Apply consistent cryptographic techniques. • Implement common naming conventions for information and systems, and maintain an integrated directory name service. • Segregate environments with different security requirements. • Control the flow of information between different environments. **11.1.4** Arrangements should be made

		countywide to provide a consistent set of rules for identifying and authenticating users, signing users on to systems and administering user access privileges. **11.1.5** Arrangements should be made enterprise-wide to provide: • Role-based access privileges. • Strong authentication for 'high-risk' users, such as system administrators.
12. System and network management	**12.1 Desktop Security** Desktop systems should be configured to function as required, and to prevent unauthorized or incorrect updates.	**12.1.1** Desktop systems should be configured in accordance with documented minimum security baseline which should cover: • Disabling or restricting particular functions or services. • Restricting access to powerful system utilities and host parameter settings. • Use of time-out facilities. • Performing key software updates. **12.1.2** Desktop Systems should be protected by the use of: • Standard, technical configurations. • A comprehensive set of system management tools. • Access control mechanisms. • Up-to-date virus protection software. • The capability to encrypt data on the hard disk. **12.1.3** Additional controls should be implemented on desktops with the capability of connecting to the Internet, by: • Using web browsers with a standard configuration • Preventing users from disabling security options in web browsers • Applying updates regularly to web browser software

		• Using personal firewalls • Warning users of the dangers of downloading mobile code and of the implications of • Accepting or rejecting 'cookies' • Restricting the downloading of mobile code.
	12.2 Server Security	**12.2.1** Server systems should be configured in accordance with documented minimum security baseline which should cover: • Disabling or restricting particular functions or services. • Restricting access to powerful system utilities and host parameter settings. • Performing key software updates. • System hardening using industry best practices **12.2.2** Server Systems should be protected by the use of: • Standard, technical configurations. • A comprehensive set of system management tools. • Access control mechanisms. • Up-to-date virus protection software. • The capability to encrypt data on the hard disk.
	12.3 Firewalls Network traffic should be routed through a firewall, prior to being allowed access to the network.	**12.3.1** A network that is linked to other networks or sub-networks (internal or external) should be protected by one or more firewalls. **12.3.2** There should be documented standards/procedures for managing firewalls, which should cover: • Filtering of specific types of traffic. • Blocking or restricting particular types or sources of traffic. • The development of pre-defined rules for filtering traffic. • Protecting firewalls against attack or

		failure. • Limiting the divulgence of information about the network. **12.3.3** Filtering of traffic should be based on pre-defined rules (or tables) that: • Have been developed by CISO and his team. • Are based on the principle of 'least access'. • Are documented and kept up-to-date. • Take account of an information security policy, network standards/procedures and user requirements.
	12.4 Secure network design The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.	**12.4.1** The design of the network should: • Incorporate a coherent, integrated set of technical standards. • Support consistent naming conventions. • Incorporate distinct sub-networks for particular groups of users or communities of interest. • Protected by firewalls. • Prevent firewalls from being bypassed. • Minimize single points of failure. • Restrict the number of entry points into the network. • Allow end-to-end network management from a primary location. • Enable the network to be remotely configured, and automatically monitored against pre-defined thresholds. • Enable network management reports and audit trails to be maintained.
	12.5 Network availability The network should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.	**12.5.1** Network facilities that are critical to the functioning of the network should be identified. **12.5.2** Single points of failure should be minimized by: • Re-routing network traffic automatically should critical

		nodes or links fail. • Providing alternative points from which the network can be administered. • Installing duplicate or alternate firewalls, main switching nodes and power supplies to critical communications equipment. • Arranging fall-back to alternative points of connection and links with external service providers. **12.5.3** The risk of malfunction of critical communications equipment, software, links and services should be reduced by: • Using only proven and up-to-date equipment, software, links and services. • Maintaining consistent versions of network equipment and software across the network. • Ensuring that key network components can be replaced within critical timescales. • Using protocols that update routing changes quickly and can withstand a high capacity of network traffic.
	12.6 Remote access All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.	**12.6.1** There should be documented standards/procedures for controlling external access to the network, which should specify: • That external connections should be identified. • That the network should be configured to restrict access. • The types of remote access connection devices permitted. • That details of external connections should be documented. • That external connections should be removed when no longer required. **12.6.2** Unauthorized external connections should be identified by:

		• Performing manual audits of network equipment and documentation to identify discrepancies with records of known external connections. • Employing network management and diagnostic tools, such as port probes and network 'discovery' tools. **12.6.3** Limited access should be given to the County network over dial-up networks. Access should be controlled and monitored using strong authentication and authorization techniques. **12.6.4** External access should be provided using a dedicated remote access server, which should: • Provide reliable and complete authentication for external connections. • Provide information for troubleshooting. • Log all connections and sessions, including details of call, start/stop time, call duration and user tracking. • Help identify possible security breaches. **12.6.5** Department must give prior approval to the connection of non-county (Vendors and others) prior to connecting to the network and ensure that: • Antivirus software is present and current. • Operating system patches are current. • Connection is discontinued upon completion of the task.
	12.7 Wireless Access Wireless access should be authorized, authenticated, encrypted and permitted only from approved locations.	**12.7.1** There should be documented standards/procedures for controlling wireless access to the network, which should cover: • Placement and configuration of wireless access points. • Methods of limiting access.

		• Use of encryption (e.g. WEP and VPN). **12.7.2** Access points should be placed within buildings, as far away from exterior walls as possible and away from sources of possible interference. **12.7.3** The network should be protected against unauthorized wireless access by using a firewall. **12.7.4** Unauthorized use of wireless access capabilities should be prevented by: • Changing security-related default access point settings. • Disabling beacons within access points that regularly broadcast the SSID. • Using IP address filtering. • Using MAC address filtering. • Using two factor authentication **12.7.5** The configuration of wireless Network Interface Cards (NIC) in client computers should be checked to ensure that they: • Do not act as access points. • Are only set-up in 'ad-hoc' mode if explicitly authorized, rather than in the standard 'infrastructure' mode. **12.7.6** Critical wireless access connections should be subject to additional security controls, including • The use of third party encryption functionality, such as a VPN. • The establishment of an authentication service.
	12.8 Secure Network device configuration Network devices should be configured to function as	**12.8.1** There should be documented standards/procedures for configuring network devices (e.g. routers, hubs, bridges, concentrators, switches and firewalls),

	required, and to prevent unauthorized or incorrect updates.	which cover: • Managing changes to tables and settings in network devices. • Restricting access to network devices. • Preventing unauthorized or incorrect updates to routing tables. **12.8.2** Network devices should be configured to: • Highlight overload or exception conditions when they occur. • Log events in a form suitable for review, and write them to a separate system. • Integrate with access control mechanisms in other devices. • Disable inessential services that are not required for the standard operation of the network. **12.8.3** Network devices should be restricted to use by authorized network staff using access controls that support individual accountability, and protected from unauthorized access.
	12.9 Network change management Changes to the network should be tested, reviewed and applied using a change management process.	**12.9.1** All types of change should be made in accordance with a change management process. **12.9.2** The change management process should be documented, and include: • Approving and testing changes to ensure that they do not compromise security controls. • Performing and signing-off changes to ensure they are made correctly and securely. • Reviewing completed changes to ensure that no unauthorized changes have been made.
	12.10 Intrusion Detection and Prevention Intrusion detection	**12.10.1** Intrusion detection methods should be employed for critical systems and

	mechanisms should be applied to critical systems and networks.	networks. The County should determine which systems and networks require protection against malicious attack and the type of attacks to be detected. **12.10.2** Intrusion detection methods should be supported by documented standards/procedures, which should cover: • Methods of identifying unauthorized activity. • Analysis of suspected intrusions. • Appropriate responses to different types of attack. **12.10.3** Intrusion detection methods should be supported by specialist software, such as Host Intrusion Detection Systems (HIDS) or Network Intrusion Detection Systems (NIDS). **12.10.4** Intrusion detection software should include: • Detection of known attack characteristics • A process for performing regular updates to intrusion detection software, to incorporate new or updated attack characteristics • Provision of alerts when suspicious activity is detected, supported by documented procedures for responding to suspected intrusions • Protection of intrusion detection mechanisms against attack, such as isolation on a separate network. **12.10.5** There should be a documented method (e.g. an escalation process) for reporting serious attacks.
	12.11 Virus Protection Virus protection arrangements should be established, and maintained	**12.11.1** There should be documented standards/procedures for providing protection against viruses, which

	countywide.	should specify: • The way in which virus protection software should be configured. • Update mechanisms for virus protection software. • A process for dealing with virus attacks. • Standardized anti-virus software **12.11.2** The risk of virus infection should be reduced by: • Installing virus protection software on servers, mail gateways, and workstations, including laptop computers and handheld computing devices. • Updating virus definitions used by virus protection software. • Distributing virus protection updates to all desktops and servers automatically and within a critical timescale. **12.11.3** Regular reviews should be performed to ensure that: • Virus protection software has not been disabled. • The configuration of virus protection software is correct. • Any updates have been applied effectively.
	12.12 Email Security E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.	**12.12.1** There should be documented standards/procedures for the provision and use of e-mail, which should specify methods of: • Configuring mail servers securely. • Scanning e-mail messages (e.g. for viruses, chain letters or offensive material). • Enhancing the security of e-mail messages. **12.12.2** Mail servers should be configured to prevent the messaging system being overloaded by limiting the size of messages/user mailboxes by restricting the

		use of large distribution lists. **12.12.3** E-mail systems should be reviewed to ensure that requirements for up-time and future availability can be met. **12.12.4** E-mail messages should be scanned for: • Attachments that could hide malicious code. • Prohibited words. • Key known phrases (e.g. those commonly used in hoax viruses or chain letters). **12.12.5** E-mail systems should be protected by: • Blocking messages that originate from undesirable web sites or list servers, to help prevent spamming. • Ensuring non-repudiation of messages, for example to prove the origin of a message, by using mechanisms such as digital signatures. **12.12.6** Standards and procedures concerning email retention, archiving and encryption should be established. **12.12.7** Anti-spam measures should be employed on County mail servers to reduce the impact of spam. **12.12.8** Anti-spam measures should be supported by documented standards/procedures, which should cover: • Methods of identifying spam email • Reduction of false positives • Support for reviewing detected spam email • Configuring filters to manage spam
	12.13 Patch management County systems should be	**12.13.1** A patch management strategy has to

	protected by timely installation of updates and patches.	be established by the County to ensure the timely installation of updates and patches to all County systems. **12.13.2** There should be documented standards and procedures that will support the patch management process. **12.13.3** The patch management process should include • Evaluate environment, risk and needs • Assign Teams responsibility • Plan release • Release development • Acceptance testing • Rollback Planning • Integration with other processes • Fair degree of automation **12.13.4** Security patches or fixes to address vulnerabilities should be: • Identified quickly. • Evaluated to determine the possible business impact of applying the patch. • Tested, and applied in a timely manner.

County of Los Angeles Accomplishments and Future Objectives

1. Security Organization

The implementation and continued operation of the County's Information Security Program requires that a security organization be established to support it. While each individual organization will have different needs, the structure that is established in each department must be aligned with the security structure for the entire County.

Organization Status and Strategy

The development and administration of an Information Security Program can only be accomplished through an organization that is dedicated to the County's security process and vision. Departments need to contribute to this organization by appointing security staff within their departments, and by appointing staff to participate in the countywide security and controls process.

The County organizational efforts are almost complete as seen in the chart below. However, not all organizations have completed their appointments and participation in the defined initiatives.

Countywide Information Security Strategy Organization Chart

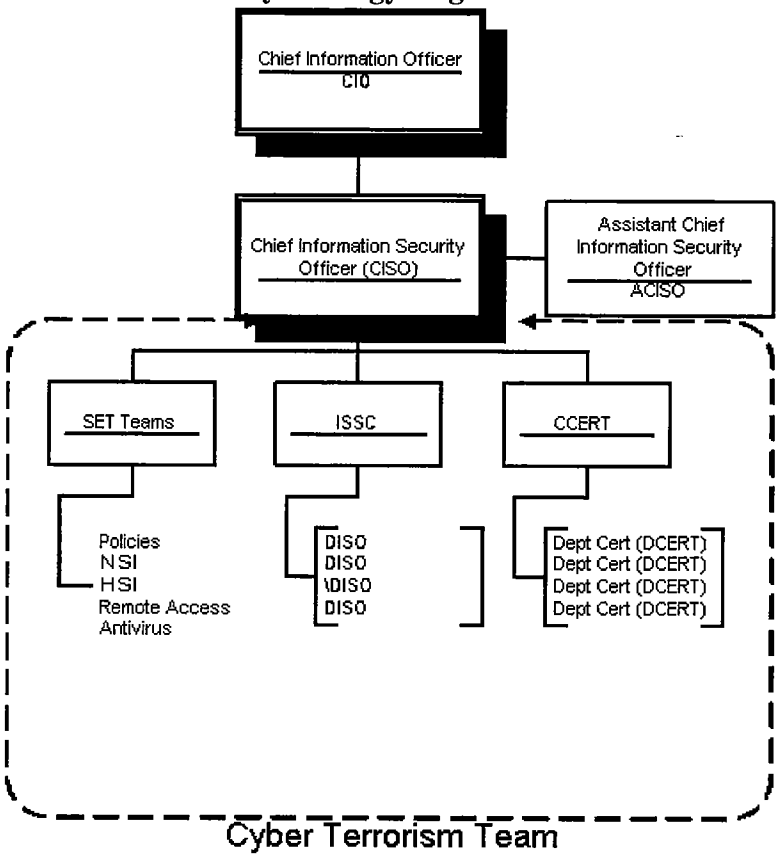

Figure 6

To provide a common approach and leadership within the County, the Chief Information Office (CIO) has established the position of Chief Information Security Officer (CISO). To assist in providing input from the various departments throughout the county, the CISO has established and conducts monthly meetings with the Information Security Steering Committee (ISSC) that consists of security representatives from the various County departments.

Chief Information Security Officer (CISO)

The Chief Information Security Officer under the direction of the CIO will:

- Develop and maintain a current information security strategy,
- Chair the Information Security Steering Committee (ISSC),
- Provide information security-related technical, regulatory and policy leadership,
- Facilitate the implementation of County information security policies,
- Coordinate information security efforts across departments,
- Lead continuing information security training and education efforts, and
- Serve as an information security resource to department heads and the Board of Supervisors.

Information Security Steering Committee (ISSC)

The Information Security Steering Committee will be composed of the Departmental Information Security Officers, the CISO and the Assistant CISO. This will provide a forum for all information security-related collaboration and decision-making. This is the deliberative body that will weigh the balance between heightened security and departments performing their individual business.

ISSC responsibilities will be to:

- Develop, review and recommend information security policies,
- Develop, review and approve best practices, standards, guidelines and procedures,
- Coordinate inter-departmental communication and collaboration,
- Coordinate Countywide education and awareness,
- Coordinate Countywide purchasing and licensing, and
- Adopt security standards.

Department Information Security Officer (DISO)

Department Information Security Officers are responsible for departmental security initiatives and efforts to comply with countywide information security policies and activities. They also represent their departments on the ISSC. To perform these duties, the DISO must be established at a level that provides management visibility, management support and objective independence. DISO responsibilities include:

- Representing their department on the ISSC,
- Developing department information security systems,
- Developing department information security policies, procedures and standards,
- Advising the department head on security related issues,
- Department security awareness programs, and
- Conducting system security audits.

Countywide Computer Emergency Response Team (CCERT)

Response to information security events that affect several departments within the County must be coordinated and planned. The CCERT was formed as a part of the Cyber Terrorism Task Force to provide that coordinated response. The CCERT is comprised of membership from the various departments and are often members of the departmental computer emergency response team (DCERT). The CCERT team meets bi-weekly to review the latest threats and ensure that membership data is kept current. The CIO's office supports this effort and requires that the CISO participate in their activities, as well as lead the response to Cyber events. Efforts will be expended in the future to improve the notification and communication process and ensure that weekend and after hour

response is viable. Additionally, training will be conducted to provide forensic capabilities to the CCERT team members.

Future Organization Activities

The security organization for the County of Los Angeles is in place and operating as planned. The Security Engineering Teams (SET) that have been defined may change as new initiatives are added and existing ones are completed.

The CCERT will continue its active role to coordinate DCERT development and to respond to incidents that occur. Future plans are to provide training and develop a core incident response team to conduct forensic analysis and investigate specific system hacks. This team also will develop improved responses through periodic exercises with scenarios that simulate various information security problems. This will assist in developing skills and keep membership contacts current.

The CISO will continue to develop the information security program through the use of committees and teams from various County organizations. ISD will provide technical support for the program with its staff. ISD Information Security and the CISO will collaborate on initiatives and funding of countywide efforts. Cooperation between these two functions is essential to success of the program.

2. Compliance and Privacy

Privacy legislation is being implemented at the State and national levels that affects the County and the information in its systems. The Health Insurance Portability and Accountability Act (HIPAA) directly applies to the Department of Health Services, the Department of Mental Health and subsets of other departments mandating them to comply with its requirements for privacy of medical records. Other privacy legislation is in process at both the State and federal levels that also will support privacy requirements. The County is currently in the process of implementing procedures to comply with HIPAA, but also is committed to implementing measures that will make it very responsive to privacy issues and the protection of personally identifiable information.

Privacy Legislation Status and Strategy

The County will implement measures to meet mandated compliance to security initiatives. However, the driver to meeting privacy legislation will be the implementation of information security practices that make sense and are cost effective to protect existing information assets. Many of the privacy requirements are in line with industry best practices related to information security and therefore will be implemented as standards. However, some privacy requirements are increasing the priority on such issues as encryption of data that is stored or being sent over communication lines. With identity

theft crimes rising at an unprecedented rate, the County of Los Angeles must take extra care to protecting personal private information for its employees and constituents. A key area being addressed by the Host Strengthening SET is standard encryption software for all portable devices as well as policies for the use of sensitive personal information.

3. User Security Awareness and Training

Effective information security programs must include user security awareness training. Training begins with employee orientation and will be conducted on a periodic basis throughout the individual's term of employment with the County. The strategy to implement an effective program is to use multiple methods for providing information, as well as formal training utilizing web-based technology and traditional classroom methods.

Periodic information security training must be provided to all system users, and should be documented to assist management in determining the effectiveness of the program. System users must certify that they have completed information security training and that they understand their role in protecting information that is entrusted to the County.

Employee Awareness Status and Strategy

The Employee Security Awareness Program will be developed and implemented through the use of automated learning management systems (LMS) as well as traditional classroom methods and published security reminders. It also will include training during employee orientation.

The goal of the program is to provide training to all employees that have access to automated information systems. Additional, and more specific, HIPAA training will be provided to employees and users of "Covered Entity" departments that include DHS, DMH, The Kirby Center, Sheriff and other entities that may be required to be HIPAA compliant.

The CIO's office is participating in the project to develop a LMS for County employee training. Information security training content will be acquired and implemented on the LMS to support the Employee Security Awareness Program. This program will require a process for acquiring specific information security content that meets specific requirements to operate on the County LMS.

Security Awareness Activities

The Security website has reached implementation and most of the content has been completed. New employee orientation material will be developed and presented during the new employee orientation process. Other media methods will be implemented as

well. The basic part of awareness will be conducted through a web-based learning management system with specific security content developed to support County issues.

4. Policies, Standards and Procedures

Policies are a key element of the County's Information Security Strategy, since they communicate the rules and responsibilities to all users of County systems as mandated by the Board of Supervisors and County management. Policies also are the basis of an employee security awareness program that communicates good security practices, as well as their responsibilities toward County management direction.

Security Policies Status and Strategy

Information security, like all major initiatives, must be supported by policy to provide direction and responsibility to the organization. Once developed, policies provide the basis for maintaining security throughout all departments of the County. The countywide policies serve as the minimum standard that must be adhered to by all. Individual organizations may need to develop more stringent policies for their specific needs or to specify controls that are not needed throughout the rest of the County. A security policy is a formal statement of the rules, which people who are given access to an organization's technology and information assets must abide.

An effective security policy must:

- Be able to be implemented through system administration procedures, publishing of acceptable use guidelines or other appropriate methods.
- Be able to be enforced with security tools, where appropriate, and with sanctions where actual prevention is not technically feasible.
- Clearly define the areas of responsibility for users, administrators and managers.
- Be communicated to all employees once they are established.
- Be flexible to the changing environments of computer networks and information technology.

Standards and Procedures

Standards are similar to policies in that they must be adhered to. They differ from policies in that they can be changed more often to meet the needs of new technology. Standards establish specific technology requirements such as minimum password rules, computer security software and network access rules. The standards for countywide use are being developed by Security Engineering Teams (SET) and accepted by the ISSC organization for use in the various departments.

Procedures must be developed by the various organizations to implement policies and standards, as well as to provide consistency in the process for administering and using

systems. Procedures contain activities that must be enforced, as well as best practices that should be implemented.

Policy Activities

The Office of the CIO will develop policies as needed to support the Board and its policy that requires a Technology and Security program. Policy development will be structured as follows:

1. The CIO/CISO will assign development of the policies to the Policy Development Team.
2. The Policy Development Team will develop the initial policy and submit to ISSC.
3. ISSC will review the policy and submit to the CIO for approval.
4. CIO will review and submit the final draft to:
    a. Department IT Managers
    b. County Counsel
    c. Employee relations
    d. BOS Audit Committee
    e. The Board for approval.
5. Publish completed policy.
6. Standards will be developed by SET teams, be approved by the ISSC, and published as attachments to existing policies after CIO approval.

5. Risk Management

Risk management begins with understanding what risks are present; what is the effect of loss and exposure; and, what is the likelihood that events will occur. When the risk of loss is understood, the risk management process determines what protections are required and develops a cost effective plan to implement them. Risk analysis and management is not a one time process since technology and organizations constantly evolve. The County must put processes in place and develop tools that can be employed when needed to maintain the process. This process must become a standard practice for all departments in the County to apply protective measures to the proper assets in a cost effective way.

6. Network Security and Access Controls

Network security and access controls are key elements for the protection of County information technology assets. These controls must encompass the entire network as well as devices that are connected to it. Controls must be in place to ensure authorization and control of external network access as well as internal. Every device on the network is a potential source of entry that must be configured with authentication and authorization in mind. Also, every server that is connected to the County's network is a

potential tool for propagation of malicious software and therefore must be properly configured with current security patches in place.

Status and Strategy

The computer networks and computing systems that have been implemented throughout the County provide connectivity to the various information systems throughout the County, as well as external entities. The strategy to protect these information assets from unauthorized access and unexpected failures includes a combination of policies, procedures and technology. It also includes the requirement to change practices that expose County computing and networking assets to risks that are present in a highly networked world.

The CIO commissioned a study to be conducted by a third party vendor to examine the County's networks and determine where vulnerabilities exist. That study showed that improved protections needed to be installed. In addition, the study demonstrated that intrusion detection and prevention was required, and resulted in the implementation of a robust network and host intrusion detection/prevention system that has proven its worth in combating attacks from worms and viruses in the past year. Improvements in deployment of the system are being implemented to further strengthen those protective measures.

Perimeter protection is provided in the form of firewalls and strong (Two-Factor) authentication for access from the outside. Modem to modem dial access, while used by many departments in the past, is not allowed unless the system requires two-factor authentication to enter, and access is restricted to specific locations. Additionally, the systems used in remote access must be equipped with antivirus software and personal firewalls. Unauthorized ISP and external network connections are prohibited. Authorized connections must be protected by County managed firewalls with intrusion detection present.

Network Access Control Actions

The County networks will receive strengthened protection through additional measures that will be implemented countywide. Internet access points will be restricted to those under ISD control with disciplined administration and protection measures in place. The Internet access points will be designed with redundancy to provide a high level of service and very high levels of security. Firewalls, intrusion detection/prevention, content controls and antivirus systems will be installed on all network-connected devices.

External connections to other agency networks also will have maximum controls installed to prevent unauthorized entry of users and malicious code using the same techniques that protect the County networks from the Internet. Users entering from these external connections will be limited to specific addresses and will be required to authenticate using digital certificates or two factor systems such as the SecurID card.

Management will implement additional network controls, which will allow controls over user visits to Internet addresses and to record abuse by users. Specific categories of w4eb access to sexually oriented sites as well as public gambling sites. Additionally, software will be implemented to control and prevent unwanted email known as spam.

7. Monitor and Audit

Monitoring and auditing of systems and applications is a required activity that will be implemented throughout the County. Network monitoring that is currently in place will be expanded to provide better coverage of the WAN and the various departmental subnets throughout the County. Automated monitoring of servers and applications must also be implemented to better support privacy requirements as well as provide forensic capabilities to determine what was accessed, who performed the action and what risks have developed as a result of the incident. Countywide monitoring must be implemented to ensure that systems are properly implemented. Departments must also implement audit processes that allow for the collection of activities as well as periodic reviews to determine if unusual activities have occurred.

8. Physical Protection of Information Assets

Physical controls over access to computing resources are just as important as control over logical or network access to computing resources. The County has a highly distributed computing environment, with various departments controlling their own computing assets and housing them in areas that may or may not be designed for that purpose. The strategy that must be employed to protect these assets includes locking rooms, which controls who can enter and monitors what is done to those assets.

Physical Protection Status and Strategy

Computing assets receive the greatest amount of protection when kept in facilities that are designed to protect them environmentally, provide redundant support and have robust access control systems that record authorized entry and provide surveillance over activities that are conducted by the authorized personnel. All critical and sensitive systems should be contained in computing centers that are designed with protection in mind.

In the event that systems cannot be located in a central secure facility, the County will improve physical access controls over critical servers through improved systems and the implementation of automated access and recording systems. Use of employee identification badges must be enforced to control access to these critical assets.

Existing Environments

Many systems for mail servers; standalone applications and PC based systems are located in departmental facilities that are not well protected. In addition, telecommunications equipment is placed in areas that can be accessed by other departments as well as other not IT staff members. The County will be attempting to improve security over these systems in the coming year and must continue to re-evaluate requirements as the systems grow and users become more dependent on them.

9. Business Continuity and Disaster Recovery

The goal of the Business Continuity Plan (BCP) is to develop procedures that can be activated to continue executing critical processes following an event that destroys or cripples the infrastructure needed to operate a business unit. This plan must include scenarios that encompass loss of the facility, systems and critical equipment. The plan also will prioritize the recovery processes for the most important processes first.

Business Continuity Status and Strategy

Business continuity planning is a proactive approach toward maintaining business activities when unexpected events cause disruption to business processes. Disaster recovery planning also is proactive in that it is geared toward restoring critical computing resources following a catastrophic event. Advanced planning may even prevent problems by assisting planners in removing risky conditions before they cause problems.

The County has developed various measures that are directed more at the restoration of systems (Disaster Recovery) than measures designed around the business processes. This weakness is being corrected under an initiative directed by the CIO office for acquiring software, consulting and developing plans for implementation by the various departments.

10. Systems Implementation and Administration

Computers that are installed in the County network must comply with standard baselines, be protected by antivirus software, be updated with all critical security patches and be maintained in accordance with the requirements that have been developed by the Host Strengthening Security Engineering Task Team. The standards are designed to provide common areas of security implementation as well as operating system-specific settings. Each computer must meet the standards that apply and be scanned for vulnerabilities before being connected to the countywide area network (WAN) or departmental LAN. In addition, the system must be periodically scanned for vulnerabilities that may have been introduced over time.

System administration also must comply with policies and standards that have been developed to govern this process. Password controls, user account management and system updates must meet security standards that have been developed for that purpose. Continued efforts from the SET teams will be required to refine the standards and controls that apply.

User administrative procedures will be strengthened to ensure that only authorized users have access to the network and systems. Administrators will be required to audit user accounts on a monthly basis and suspend or delete any accounts that have not been used in the last 90 days. Additionally, actual employee data will be compared to the account files to ensure that only authorized users are granted access.

Desktop and Laptop Systems

Increasingly destructive worm attacks have demonstrated that personally assigned computers on desktops and mobile laptop devices are a threat to the County's networks due to their large numbers when infected. These attacks can create a denial of service situation when infected machines begin to emit large volumes of messages into the network. Because of that risk, a desktop strategy must be implemented that is designed to prevent worm and hacker attacks. The defenses that are employed require that these systems be automatically updated with critical system patches as well as antivirus software. In addition, intrusion prevention software must be employed to prevent day zero attacks where a signature of the malicious code has not been developed before the attack.

Software vendors are developing tools that will allow the verification of healthy systems whenever they are connected to the network. This verification must be employed to check internal connections of systems as well as those originating from external sources. Where the system is not current, the user will be denied network access until they have completed the latest updates from officially approved sources in the County. Computers with outdated and unsupported operating systems will be denied access to the network.

Los Angeles County Information Security Milestones and Accomplishments

Milestone/Accomplishments	Status	Date	Strategy
CISO/CIPO/ACISO	Complete	11/02	**1.1** Security Management and Organization
Steering Committee	Complete	10/02	**1.2** Security Management and Organization
Computer Emergency Response Teams	Complete	11/03	**1.2** Security Management and Organization
ISSC Meetings	Ongoing	10/2002	**1.2.2** Security Management and Organization
Privacy of HIPAA information	Ongoing	12/01/2007	**2.1.4** Compliance and privacy
HIPAA privacy assessments	Ongoing	07/31/2006	**2.1.5** Compliance and privacy
Information Security Web Site	Complete	03/06	**3.1.2** User Security Awareness and Training
Wireless LAN Guidelines	Completed	3/13/2003	**4.1.5** Policy, standards and procedures
Board Policy (Master Policy)	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Internet Usage Security Policy	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Use of County Information Technology Resources	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Countywide Antivirus Security Policy	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Use of Electronic Email by County Employees	Completed	7/13/2004	**4.1.5** Policy, standards and procedures

Milestone/Accomplishments	Status	Date	Strategy
Information Technology Risk Assessment	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Auditing and Compliance Policy	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Countywide Computer Security Threat Response	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Physical Security	Completed	7/13/2004	**4.1.5** Policy, standards and procedures
Network Infrastructure Device Security	Completed	5/6/2003	**4.1.5** Policy, standards and procedures
Minimum Standards for Configuring Antivirus Software for Windows Server	Completed	11/19/2003	**4.1.5** Policy, standards and procedures
MS Windows 2000 Server Baseline Security Standards	Completed	11/19/2003	**4.1.5** Policy, standards and procedures
MS Windows XP	Completed	6/30/2005	**4.1.5** Policy, standards and procedures
MS Windows 2003	Completed	6/30/2006	**4.1.5** Policy, standards and procedures
Patch Management Software Standard	Completed	1/25/2005	**4.1.5** Policy, standards and procedures
CCERT Computer Security Threat Response	Completed	4/1/2003	**4.1.5** Policy, standards and procedures
HIPPA Risk Analysis	Complete	10/15/2005	**5.1** Risk Mgmt
Ensure that users of County information systems are identified and authenticated	Completed	Ongoing	**6.1.1** Access Control
Utilize two factor authentication for system administrators	Completed	6/2002	**6.1.2** Access Control
Ensure that users do not share userids	Completed	7/2004	**6.1.3** Access Control

Milestone/Accomplishments	Status	Date	Strategy
Authorize and ensure users of County systems are authorized before granting access	Completed	7/2004	**6.2.1** Access Control
Document user authorization process	Completed	3/2001	**6.2.2** Access Control
Business Continuity Planning	BIA complete Departmental plans in process	12/31/2003	**9.3.2** Business Continuity Planning and Disaster Recovery
Desktop Standard Security	Complete	3/2002	**12.1.1** System and Network Management
Desktop Security and Antivirus	Complete	3/2002	**12.1.2** System and Network Management
Desktop Protection Methods	Complete	3/2002	**12.1.3** System and Network Management
Standard Server Templates and Baselines	Complete	11/18/04	**12.2.1** System and Network Management
Standard Server Templates	XP complete	1/05	**12.2.2** System and Network Management
Firewall Protections	Complete	3/2002	**12.3.1** System and Network Management
IDS and Event Correlation	Complete	2/2004	**12.3.3** System and Network Management
Secure Network Design	Complete	3/2002	**12.4.1** System and Network Management
Wireless Security Standards	Complete	2/2005	**12.7.1** System and Network Mgmt
Access Point Controls	Complete	2/2005	**12.7.2** System and Network Mgmt
Firewall Controls	Complete	2/2005	**12.7.3** System and Network Mgmt

Milestone/Accomplishments	Status	Date	Strategy
Wireless Implementation Standards	Complete	2/2005	**12.7.4** System and Network Mgmt
NIC Card Controls	Complete	2/2005	**12.7.5** System and Network Mgmt
VPN Controls Where Required	Complete	2/2005	**12.7.6** System and Network Mgmt
Documented Standards for Network Devices	Complete	2/2002	**12.8.1** System and Network Mgmt
Network Device Logging and Visibility	Complete with CIC	2/2004	**12.8.2** System and Network Mgmt
Protect from Unauthorized Access	Complete	2/2004	**12.8.3** System and Network Mgmt
Network Change Management	Complete by ISD	2/2004	**12.9.1** System and Network Mgmt
Change Management Process	Complete	2/2004	**12.9.2** System and Network Mgmt
Intrusion Detection Plan	Complete	2/2004	**12.10.1** System and Network Mgmt
IDS Documentation	Complete	2/2004	**12.10.2** System and Network Mgmt
IDS and Prevention in Place	Complete	2/2004	**12.10.3** System and Network Mgmt
IDS kept Current	Complete	2/2004	**12.10.4** System and Network Mgmt
CCERT Process	Complete	2/2004	**12.10.5** System and Network Mgmt
Antivirus Documentation	Complete	7/2004	**12.11.1** System and Network Mgmt

Milestone/Accomplishments	Status	Date	Strategy
A/V Installed and Current	Complete	7/2004	**12.11.2** System and Network Mgmt
A/V Verification	Complete	7/2004	**12.11.3** System and Network Mgmt
Email Security Policy	Complete	7/2004	**12.12.1** System and Network Mgmt
Email Server Configuration Standard	Complete	7/2005	**12.12.1** System and Network Mgmt
Mail Server Configuration	Departmental Options	N/A	**12.12.2** System and Network Mgmt
Mail Server Performance Monitoring	Departmental Options	N/A	**12.12.3** System and Network Mgmt
Anti-spam Software	Brightmail	7/2005	**12.12.4** System and Network Mgmt
Anti-spam Implementation	Brightmail	7/2005	**12.12.5** System and Network Mgmt
Email Retention Standards	CAO Developing	N/A	**12.12.6** System and Network Mgmt
Antispam Deployment	Brightmail	7/2005	**12.12.7** System and Network Mgmt
Antispam Documentation	Departmental	N/A	**12.12.8** System and Network Mgmt
Patch Management Software	Complete	07/2004	**12.13.1** System and Network Mgmt
Patch Management Standard	Complete	12/2004	**12.13.2** System and Network Mgmt
Patch Management Process	Complete	12/2004	**12.13.3** System and Network Mgmt

Milestone/Accomplishments	Status	Date	Strategy
Patch Installation Decision	Departmental Standard	6/2004	**12.13.4** System and Network Mgmt

I. Future Objectives

Milestone/Accomplishments	Status	Date	Strategy
Implement HIPPA Security	In Process	07/07	**2.1.1** Compliance and Privacy
Establish committee or appoint an individual for privacy issues	Need to appoint a County Privacy Officer	3/30/07	**2.1.1** Compliance and privacy
Documented standards/procedures for information privacy	Awaiting Privacy Officer	3/30/07	**2.1.2** Compliance and privacy
Security Awareness Program	In Progress	3/30/07	**3.1,1** User Security Awareness and Training
Monitor and measure security awareness training	LMS implementation will allow mgmt to monitor progress of departments	2/28/2007	**3.1.3** User Security Awareness and Training
Security awareness policy	In Progress	02/15/07	**3.1.4** User Security Awareness and Training
Develop and acquire content for security awareness curriculum for IT staffs	Security awareness curriculum in progress	4/15/2007	**3.2.1** User Security Awareness and Training
Define security training curriculum for various IT job classifications to include system developers	Security awareness curriculum in progress	4/15/2007	**3.2.2** User Security Awareness and Training
Work with HR to implement a County security certification program to support training	Will be developed based on curriculum completion	7/31/2007	**3.2.3** User Security Awareness and Training

Milestone/Accomplishments	Status	Date	Strategy
Information Technology Disaster Recovery Policy	Under revision with SET	3/30/2007	**4.1** Policy, standards and procedures
Information Technology Business Continuity Policy	Under revision with SET	3/30/2007	**4.1** Policy, standards and procedures
Security Training and Awareness Policy	Routing	02/15/2007	**4.1** Policy, standards and procedures
Data Disposal Policy	In ISSC	3/30/2007	**4,1** Policy, standards and procedures
Software Security Policy and Standard	Set Team	6/1/2007	**4,1** Policy, standards and procedures
Portable Devices/Storage Media Security Policy	With CIO	02/1/2007	**4.1** Policy, standards and procedures
Data Classification and Protection Policy	With CAO	9/1/2007	**4.1** Policy, standards and procedures
Incident Response Policy	Routing	02/15/2006	**4.1** Policy, standards and procedures
Network Security Policy	In Progress	7/1/2007	**4.1** Policy, standards and procedures
Information Security Risk Assessment countywide	Future Objective	11/30/2007	**5.1.1** Risk Management
Analyze Business risks associated with County systems	Required by Board Policy 6.107 for each department	6/30/2007	**5.1.2** Risk Management
Develop consistent standards to apply to the risk analysis process	Auditor-Controller to document the process according to policy	6/30/2007	**5.1.3** Risk Management
Develop a method to document the risk results with identification of key risks and recommended actions	Auditor-Controller to document the process according to policy	6/30/2007	**5.1.4** Risk Management
Implement user provisioning system that provides portal access to new passwords	ISD in process	05/01/2007	**6.1.4** Access control

Milestone/Accomplishments	Status	Date	Strategy
Develop standards to require the proper addition, access control, and timely deletion of user access credentials	SET team development	11/30/2007	**6.1.5** Access control
Develop standards to require logging of user accesses	SET team development	7/31/2007	**6.1.6** Access control
Develop Digital Signature capability	PKI Initiative	12/31/07	**6.1.7** Access Control
Develop an enterprise Active Directory and utilize the HR database to perform enterprise wide ID deactivation	ISD Active Directory project in process	6/01/2007	**6.2.3** Access control
Develop standards that regulate 3rd party access	SET team	08/01/2007	**6.3.1** Access control
Develop standard contract language that provides 3rd party control and liability limitations for system access	CISO office to develop language	6/30/2007	**6.3.2** Access Control
Develop methods to authenticate 3rd party access and restrict to least privilege needed	NAC and Active Directory initiative	08/01/2007	**6.3.3** Access Control
Automated Policy Enforcement (technology)	Future Objective	11/1/2007	**7.1.1** Monitor and Audit
Security Dashboard	In Progress	6/30/2007	**7.1.5** Monitor and Audit
BCP Plans	Departments training and planned development	12/31/07	**9.3.3** Business Continuity Planning and Disaster Recovery
BCP service priority list and key tasks	Departments training and planned development	12/31/07	**9.3.4** Business Continuity Planning and Disaster Recovery
BCP Provisioning list	Departments training and planned development	12/31/07	**9.3.5** Business Continuity Planning and Disaster Recovery

Milestone/Accomplishments	Status	Date	Strategy
BCP Testing	Test plan and actual testing when plans complete	6/01/08	**9.3.6** Business Continuity Planning and Disaster Recovery
Documented System Development Methodology	Application SET team	12/01/07	**10.1.1** Application and system development
Secure system development lifecycle guideline	In process with SET team	03/31/07	**10.1.2** Application and system development
Secure System Development Methodology	In process with SET team	7/31/07	**10.1.3** Application and system development
Maintain development methodology	As required when established	TBD	**10.1.4** Application and system development
Monitor Compliance	As required when established	TBD	**10.1.5** Application and system development
Development Environments	Departmental effort to be defined	12/31/07	**10.2.1** Application and system development
Development Environment Isolation	Departmental effort to be defined	12/31/07	**10.2.2** Application and system development
Development Environment Protection Measures	Departmental effort to be defined	12/31/07	**10.2.3** Application and system development
Development Environment Key Asset Protection	Departmental effort to be defined	12/31/07	**10.2.4** Application and system development

Milestone/Accomplishments	Status	Date	Strategy
Security in the Design Phase	In process with the SET team	7/31/07	**10.3.1** Application and system development
System Design Security Requirements Defined	In process with the SET team	7/31/07	**10.3.2** Application and system development
Evaluate System Alternatives in the Life Cycle	In process with the SET team	7/31/07	**10.3.3** Application and system development
Document and Verify System Design	In process with the SET team	7/31/07	**10.3.4** Application and system development
Document and Verify System Design Application Controls	In process with the SET team	7/31/07	**10.4.1** Application and system development
Document and Verify System Design Security Controls	In process with the SET team	7/31/07	**10.4.2** Application and system development
Document and Verify System Design Detailed Security Controls	In process with the SET team	7/31/07	**10.4.3** Application and system development
Document and Verify System Build	In process with the SET team	7/31/07	**10.5.1** Application and system development
Document and Verify System Build Standards	In process with the SET team	7/31/07	**10.5.2** Application and system development
Document and Verify System Build Inspection Process	In process with the SET team	7/31/07	**10.5.3**Applicatio n and system development
Document and Verify System Build Best Practices and Tools	In process with the SET team	7/31/07	**10.5.4** Application and system development

Milestone/Accomplishments	Status	Date	Strategy
Document and Verify System Build Modifications	In process with the SET team	7/31/07	**10.5.5** Application and system development
Web Development Additional Controls	Assigned to Application SET team	10/31/07	**10.6.1** Application and system development
Web Development Privacy Policy	Assigned to Application SET team	10/31/07	**10.6.2** Application and system development
Web Server Security	Assigned to Application SET team	10/31/07	**10.6.3** Application and system development
Web Server to Back Office Server Security	Assigned to Application SET team	10/31/07	**10.6.4** Application and system development
Web Site Design Controls	Assigned to Application SET team	10/31/07	**10.6.5** Application and system development
Define Transaction Processing Monitors	Assigned to Application SET team	10/31/07	**10.6.6** Application and system development
Provide Encryption for In Transit Sensitive Data	Assigned to Application SET team	10/31/07	**10.6.7** Application and system development
Define System Testing in Development	Assigned to Application SET team	10/31/07	**10.7.1** Application and system development
Define System Testing in Development Standard Procedures	Assigned to Application SET team	12/31/07	**10.7.2** Application and system development

Milestone/Accomplishments	Status	Date	Strategy
Define System Testing in Development for Go Live	Assigned to Application SET team	12/31/07	**10.7.3** Application and system development
Test Plan Documentation Templates	Assigned to Application SET team	12/31/07	**10.7.4** Application and system development
Define Test Areas	Assigned to Application SET team	12/31/07	**10.7.5** Application and system development
Select Automated Tools for System Testing	Assigned to Application SET team	12/31/07	**10.7.6** Application and system development
Hardware Acquisition Standards	Assigned to Application SET team	12/31/07	**10.8.1** Application and system development
Hardware Selection Procedures	Assigned to Application SET team	12/31/07	**10.8.2** Application and system development
Utilize Third Party Hardware Ratings	Assigned to Application SET team	12/31/07	**10.8.3** Application and system development
Hardware Review Procedures for Staff	Assigned to Application SET team	12/31/07	**10.8.4** Application and system development
Develop Software Procurement Language	Assigned to CISO Staff	03/31/07	**10.8.5** Application and system development
Establish an Information Security Architecture	In Process	1/31/07	**11.1.1** System Architecture and Design
Establish a Countywide Process for Consistent Security Mechanisms	Continued Standards Development	7/01/07	**11.1.2** System Architecture and Design

Milestone/Accomplishments	Status	Date	Strategy
Enterprise System Arrangements	Security Architecture Document	1/31/07	**11.1.3** System Architecture and Design
Enterprise Identity Management	Future project	1/31/08	**11.1.4** System Architecture and Design
Enterprise Role Based Authentication Process	Enterprise Directory in process	7/01/07	**11.1.5** System Architecture and Design

VI. The Information Security Scorecard

The information Security Scorecard is an attempt to create a common measurement structure across the County and to simplify data collection. The CISO can benefit substantially by working with different process groups within the County to help derive these metrics.

Deriving key performance indicators (PKI) for Information Security is similar to defining them for other business processes like total quality management. The Information Security Scorecard (ISS) provides a framework for performance data to be gathered and then benchmarked against internal and eventually external operations. The KPI categories are those set out in our framework:

- Organization,
  -
- People,
  - Employees as a component of the projects success
- Process,
  - Security Processes as a component of the project's success.
- Technology,
  - Security products or serves deployed to enable the projects success.
- and Cost
  - Cost of the Security, Project Cost, Productivity loss for time lost.

Functional Domains

The functional domains for measurement reflect those that we determined to be the essential topic areas for the County IS. Continuous programs immediately lend themselves to measurement and tracking – such as User Awareness Training, Patch Management, Audit Management and Regulatory Compliance, to name a few. Fixed length projects can form independent functional domains, which would then translate to continuous measurement areas once the project is complete and the solution is in process. Similarly, some of the performance metrics used to justify the project can be used to measures compliance or performance beyond project completion. It should be clear that each Function Domain will have multiple sub-domains for which measurements can be made that reflect the different functional responsibilities contained within the domain.

Performance Dimensions

The KPI being tracked will reflect performance in one of three dimensions –

1. Performance – how well are we doing?
2. Value – What is the value to the relevant stakeholder?
3. Relative Performance – How are we doing with respect to peers?

An example would apply to User Security Awareness. For the different performance dimensions, performance could be expressed as the percentage of employees trained on security matters. The value could be a measure of reduced downtime from security

vulnerabilities, expressed as the percent of progress towards a specific goal. The relative performance measure could compare the percent of employees trained in a particular group to that of other groups in the county. Remember these measurements represent an aggregate across all initiatives targeted to improve User Security Awareness.

The resulting ISS can be used to compare departments within the county and later compare agencies across the county.

	Category														
	Organization			People			Process			Technology			Cost		
Performance Dimension	P	V	RP	P	V	RP	P	V	RP	P	V	RP	P	V	RP
Functional Domain															
Security Management and organization															
Compliance and Privacy															
User security awareness and training															
Security Policy, Standards & procedures															
Risk Management															
Access Control															
Monitor and Audit															
Physical Security															
Business Continuity															
Application and Systems Development															
System architecture and design															
System and Network Management															